Smart Card and Mobile Phone Based Business Models for Financial Inclusion

P.K.Patel

AGM,MoF

BC Model & Technologies

- Smartcard Based Model
- Mobile Phone based Model
- Internet Based Model
- Aadhaar enabled Model
- Hybrid Model

•highly secure;

•amenable to audit; and

•follow widely accepted open standards to allow inter-operability among the different systems adopted by different banks.

Selection of Technology

- **Secure**
  - ✓ Supports two factor authentication (Card & Biometric)
- **Scalable**
  - ✓ Capability to handle multiple products & Services
- **Reliable**
  - ✓ Transactions are secure and ensures non-repudiation
- **Flexible**
  - ✓ Supports multiple connectivity and power options
- **Interoperable**
  - ✓ Customers can transact from the branch or other BCs
- **Robust & Upgradable**
  - ✓ Supports contact, Contact less and mag-stripe interfaces
- **Cost Effective**

Smart Card

1) A **smart card**, **chip card**, or **integrated circuit card** (**ICC**), is any pocket-sized card with embedded integrated circuits. There are two broad categories of ICCs.

2) Memory cards contain only non-volatile memory storage components, and perhaps dedicated security logic. Microprocessor cards contain volatile memory and microprocessor components.

3)The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate **.**

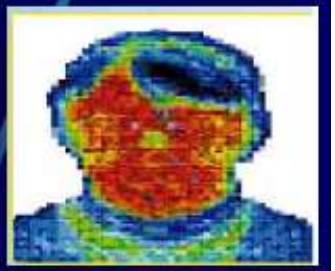
4) Contact (ISO 7816) and Contactless Card (ISO 14443)

Different Biometrics

Finger print

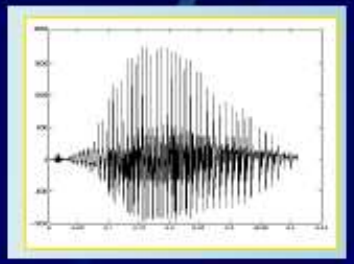
Face

Iris



Facial Thermogram

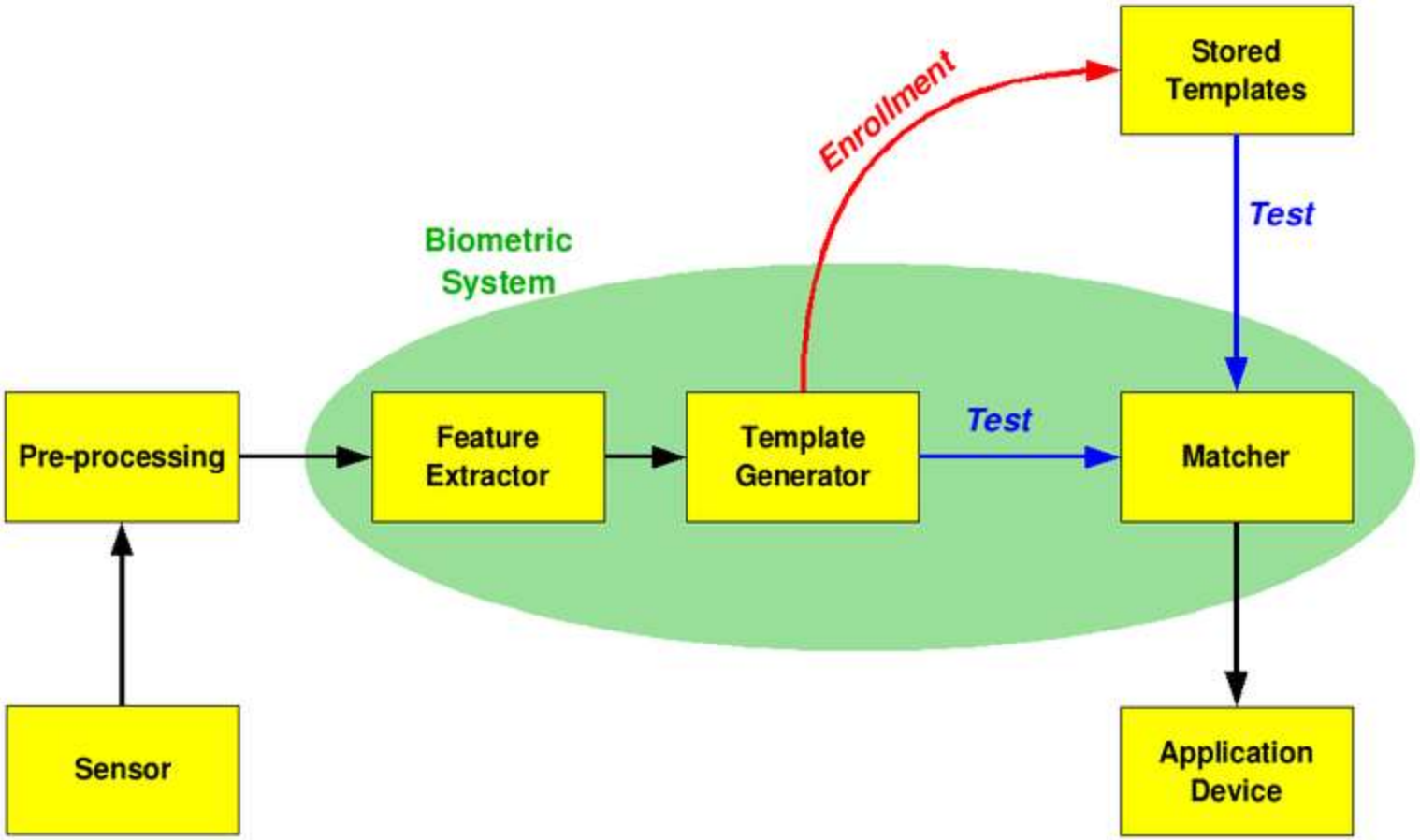
Palmprint



Voice

Signature

The basic block diagram of a biometric system



POS (1)

1	Side Panel	7	Printer
2	Power Cable	8	Paper Feed Button
3	Antenna for GPRS Connection	9	Status Indicators
4	Display Screen	10	Fingerprint Sensor
5	Key Pad	11	Contactless Card Slot
	Paper Holder	12	Contact Card Slot

कृषि बैंकिंग महाविद्यालय
College of Agricultural Banking
(An ISO 9001: 2000 Certified Training Institute of Reserve Bank of India)

Device Characteristics

- Card Based Device
- Support for Fingerprint Authentication
- Redundant Power Sources for continuous operation
- Mobile and easy to carry
- Voice Guidance in Local Language
- Support for multiple communication Channels
- Capability to support multiple power sources
- Device stores only minimal data
- Ability to handle multiple products and services
- Receipt printing
- Scalable

Banking Ecosystem

Bank Core Servers/TBA Servers

Account Management
Interest Runs
Interface to Banking Network

Identity Management System


Printer


IMS Server


Biometric Capture

Customer Creation
Biometric and KYC Capture
Account Creation
Personalised Card Issue
Automatic Fingerprint Matching

Personalised Card Issued to Customer

Secure protocol for customer account information exchange
- **ISO 8583 standard messaging**
- **Bank-defined proprietary messaging**

- Biometric Authentication and Mediation Services
- Transaction Services
- Account Information
- Synchronisation Services - Interface between Bank Server and Point of Service
- Card Management
- Branch and BC MIS
- Settlement Systems

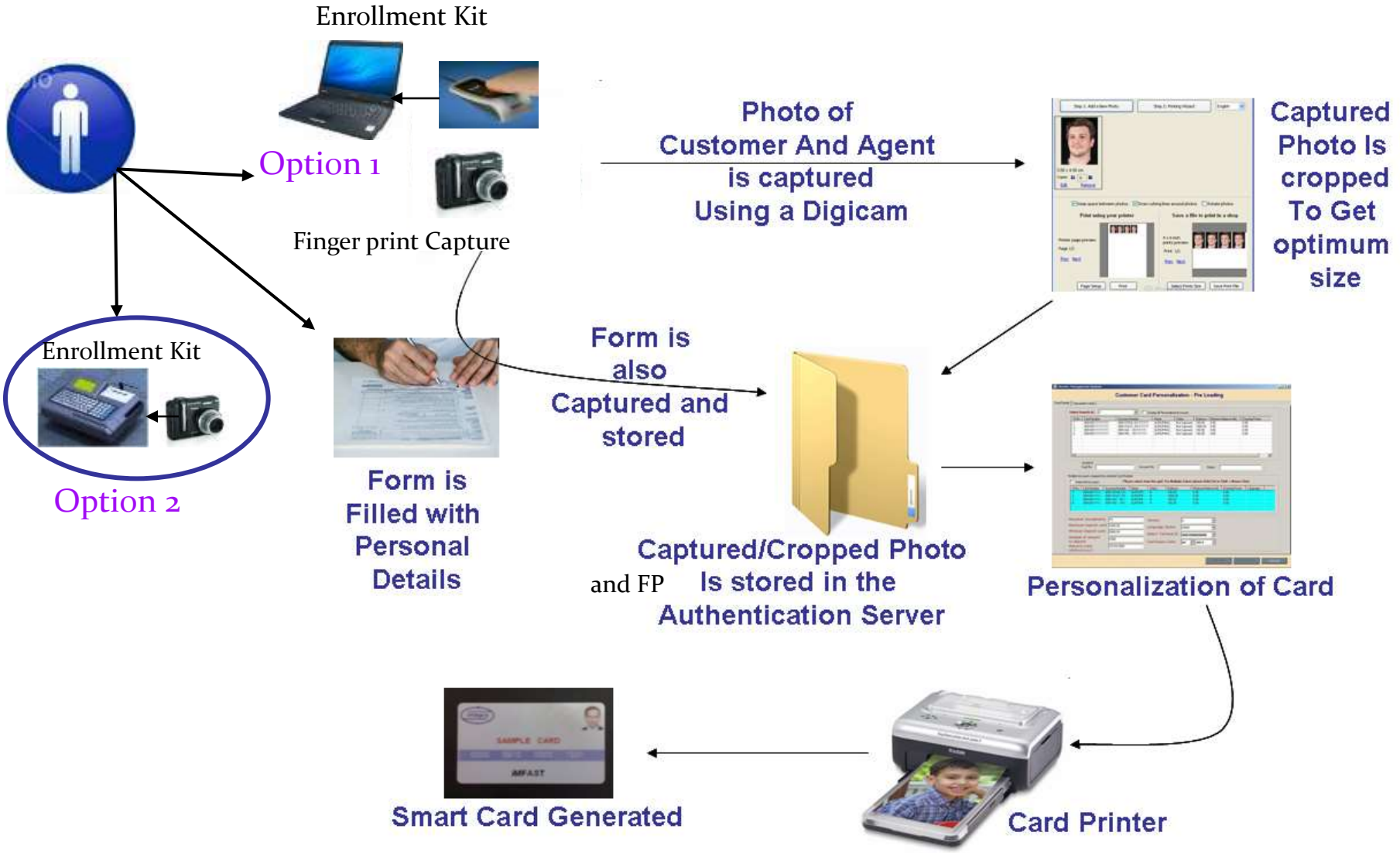
Backend Gateway and Server

Offline mode transactions and synchronisation

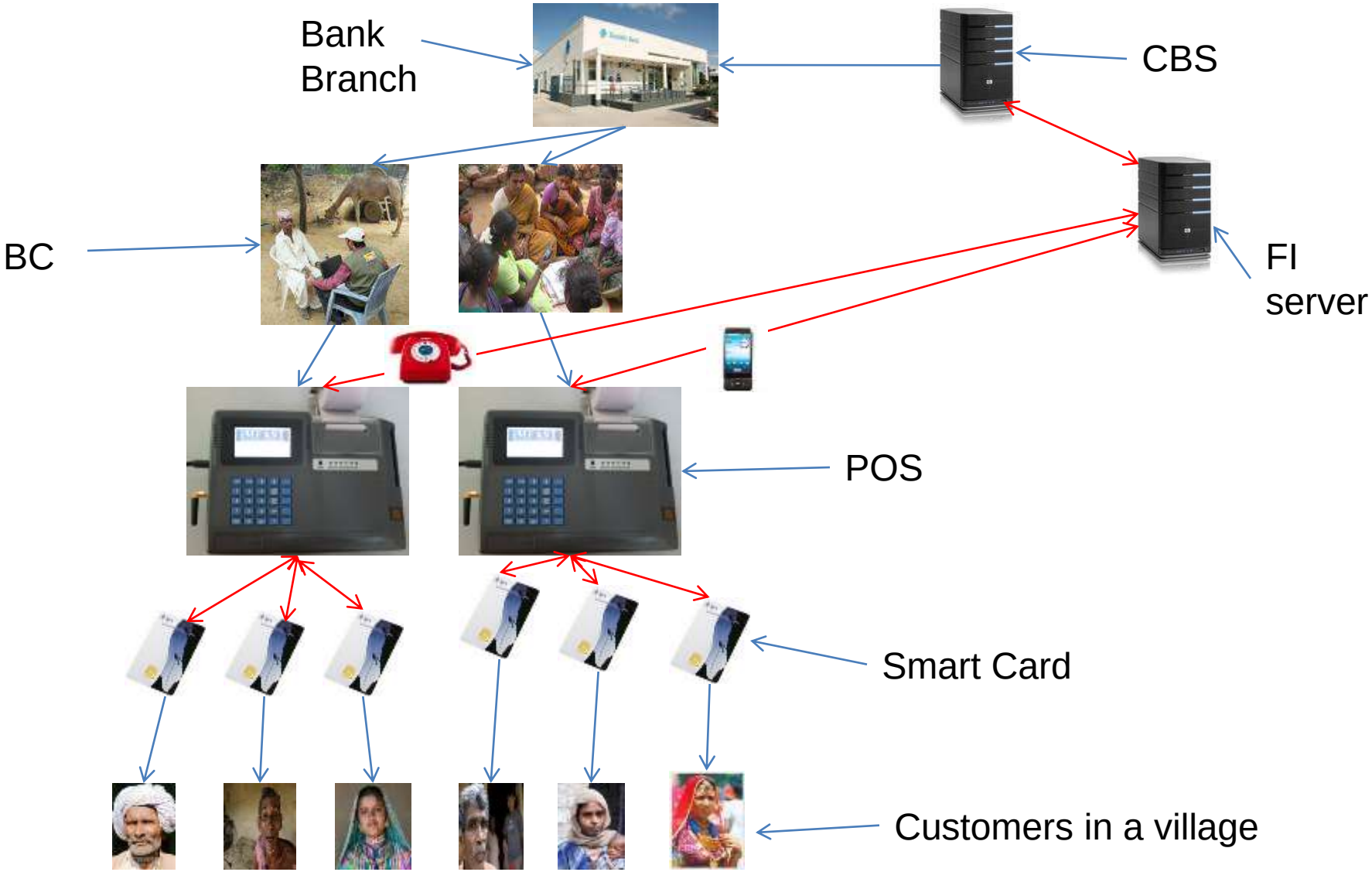
Online mode transactions

Cash Deposit
Cash Withdrawal
Balance Enquiry
Mini Statement
Other Services

Rural Touch Point


Enrollment Kit
Option 1
Finger print Capture
Photo of
Customer And Agent
is captured
Using a Digicam
Captured
Photo Is
cropped
To Get
optimum
size
Enrollment Kit
Option 2
Form is
Filled with
Personal
Details
Form is
also
Captured and
stored
Captured/Cropped Photo
and FP Is stored in the
Authentication Server
Personalization of Card
Smart Card Generated
Card Printer

BC Transaction Model



Future Scenario

POS

ISO

8583

NFS

Inter
Bank
Clearing
And
Settlement
System

Standardization

- The Smart Card Numbering Scheme
- The Smart Card Operating System
- The FI Customer Card Data Architecture
- The FI Terminal Operator Card Data Architecture
- The Terminal Functionality Specification
- Key Management System

Card Numbering Scheme

- Length of the card number: 19 Digits
- 9 – National Scheme
- 356 – Country Code
- XXXX – Bank Identification Number*
- XXXXX – Branch Code*
- XXXXX – Card Serial Number*
- X – Checksum (Luhn’s algorithm)

Terminal Functionality Specifications

- **Minimal Functionality that should be supported**
- DEPOSIT
- WITHDRAWAL
- BALANCE ENQUIRY
- MINI STATEMENT
- **Full Functionality (optional)**
- FUNDS TRANSFER/ REMITTANCES
- BILL PAYMENTS
- LOANS
- INVESTMENTS (TERM DEPOSITS, FDS, RDS ETC.)
- **Extended Functionality**
- MUTUAL FUNDS
- INSURANCE (LIFE, HEALTH, CROP, ETC.)
- PENSIONS

Standards for POS Terminal

- Security Aspects
  - Once the application is loaded on the device there should be no possibilities to modify the application at the field. Reloading or modifying of application should be possible only by an authorized agency or the bank.
  - Fingerprint matching (1:1) – Fingerprint image shall be captured live which shall be matched with fingerprint stored in the card. Matching algorithm can be implemented by the manufacturers with high level of accuracy.
  - Connectivity of terminal to backend protected through SSL/PKI
  - The terminal will have provision for a SAM card. The flash memory can be used for storing BOD file, data downloaded from back end, transaction data etc. in an encrypted form. SAM is for authentication and not storage.

Smart Card Security

- Mutual authentication between card and terminal using Triple-DES.
- Cardholder verification using biometric authentication – the fingerprint stored on the card is to be encrypted to prevent misuse. The fingerprint images are to be stored in WSQ format.

Key Management System

- Generation of Parent/Seed Keys (Three of Five Scheme) and their safe storage and Usage.
- Generation of Master Keys and production of Master Key based Authority Cards.
- Key Diversification from Master keys and safely injecting them to the FI Customer Cards to activate them.
- Providing an External Authentication Protocol to perform authentication of FI Customer Card.
- Providing an External Authentication Protocol to perform Role Authentication before Field Transaction by a BC.
- Providing an External Authentication Protocol to perform Role Authentication before allowing to load a new application.
- Providing a Mutual Authentication Protocol between FI Customer Card & BC Card .

Smart Card

FOR

- Highest level of security
- It is the future with ‘Aadhar’ coming in
- Open standards available for interoperability

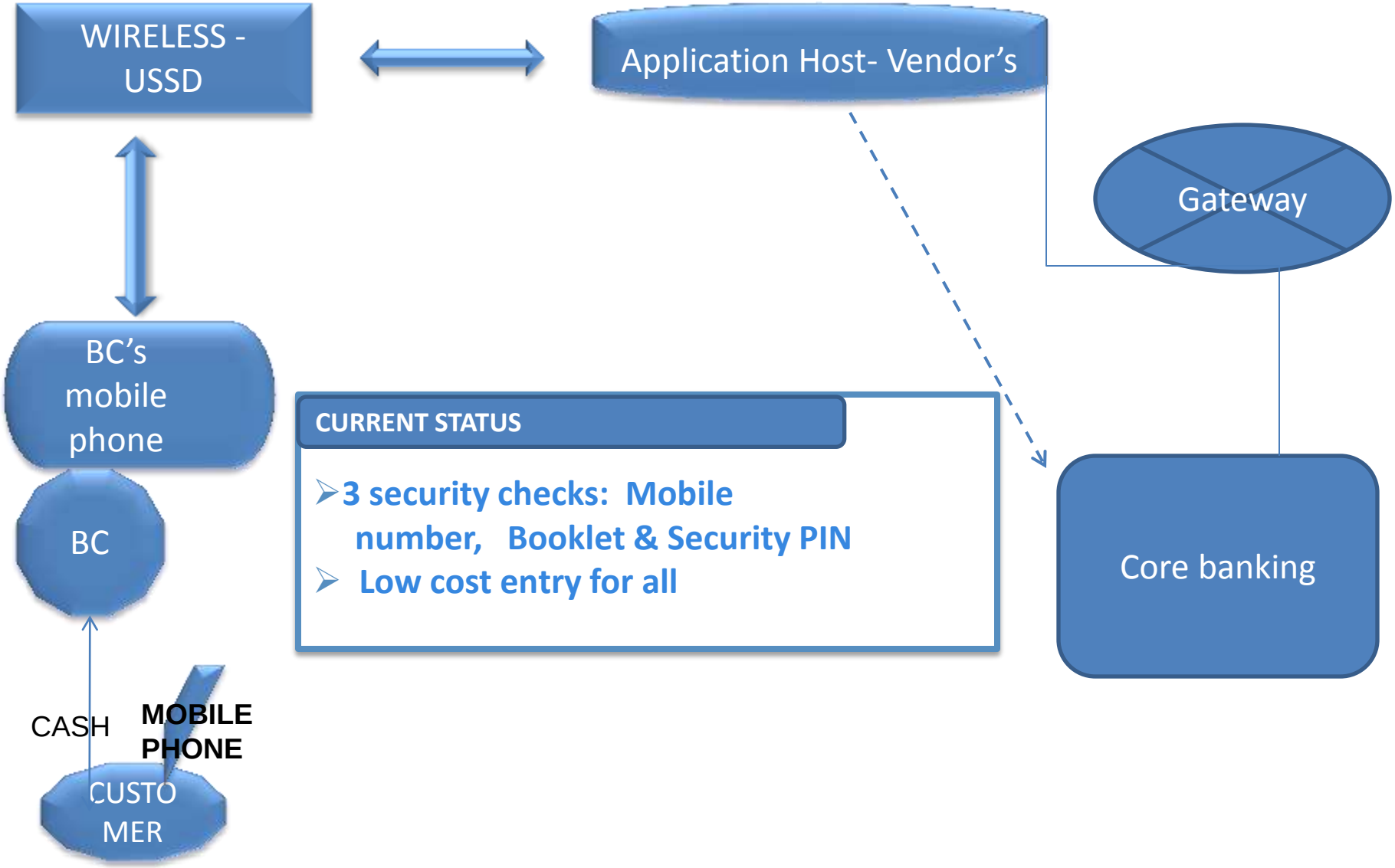
AGAINST

- Vendors / products not fully tested.(transactional ability/ scalability)
- Issues with hardware / card delivery & quality ,delays the process
- Support and maintenance of equipment at BC points
- It’s a New system – training required for Customer, BC and Branch staff
- High Capital and running cost could impact viability.
- Banks will have to upgrade ATM’s in due course

All-purpose Single Card

- Presently, various types of cards are floated by various Banks.
- Debit Cards, Credit Cards, KCC, GCC etc.
- Card to contain the full particulars of the account holder with limits sanctioned/ available, balance outstanding, photo, finger prints, etc. with provision for data updation and the UID no.
- Cover working capital, consumption loan and OD Limits
- Card should be operable both in online and offline systems
- Operable in ATMs/POS/POTs
- Contactless smart card chip must be conforming to the necessary security standards

TECHNOLOGY INITIATIVES : Process – MOBILE BASED



NFC – How it operates?

IMmediate Payment Service

- IMPS funds transfer (P2P)
  - IMPS funds transfer using Mobile Phone
  - IMPS fund transfer using ATM/Internet banking channel
- IMPS funds transfer through Account Number/IFSC
- IMPS Merchant Payments
- National Unified USSD Payments

IMmediate Payment Service

IMPS funds transfer through Account Number

Following details are required to entered

- Beneficiary account number
- Beneficiary IFSC code
- Account type (optional)
- Amount
- M-PIN
- Remarks

एको /– pioneers in use of Mobile

- Eko is the BC of SBI, ICICI Bank and Yes Bank
- Enables instant financial transactions & money transfer
- Money transferred into bank account
- HQ at Delhi with operations over 7 states

Mobile Kisan Credit Card

- Launched in Villupuram dist of TN by Pallavan Gramin Bank
- Use mobile phones for purchasing farm inputs, cash withdrawal and deposits
- PGB uses SMS and IVR facility through a partner PayMate

Mobile Wallets

- Semi-closed payment options
- Airtel Money one of the pioneers
- Allow mobile recharges, bill payments, DTH recharges, shopping, book tickets
- Tied up with Axis Bank for basic banking account with mobile facility
- Limits upto Rs 10,000

Airtel Money

Short Messaging Service (SMS)

- SMS allows wireless transfer of text upto 160 characters between cell phones
- From phone message goes to a SMS center (SMSC)
- Low security due to unencrypted storage in senders phone
- Limited query based usage
- Customer needs to know the exact syntax of SMS

Wireless Application Protocol (WAP)

- WAP is a technical protocol for accessing internet
- Mobile based browser
- Internet banking accessed through mobile
- Same security features as internet banking
- Anti-virus for phones?
- Connectivity issues?

Voice Channel (IVRS)

- Voice channel uses basic functionality of phones
- Menu driven interface
- Dialects, complicated menu options, long transactions times – impeding factors

SIM Toolkit Applications (STK)

- Application code embedded in mobile SIM card
- Independent of phone or network
- Mobile banking application would be implemented utlizing the STK builder
- Possible to embed higher security features

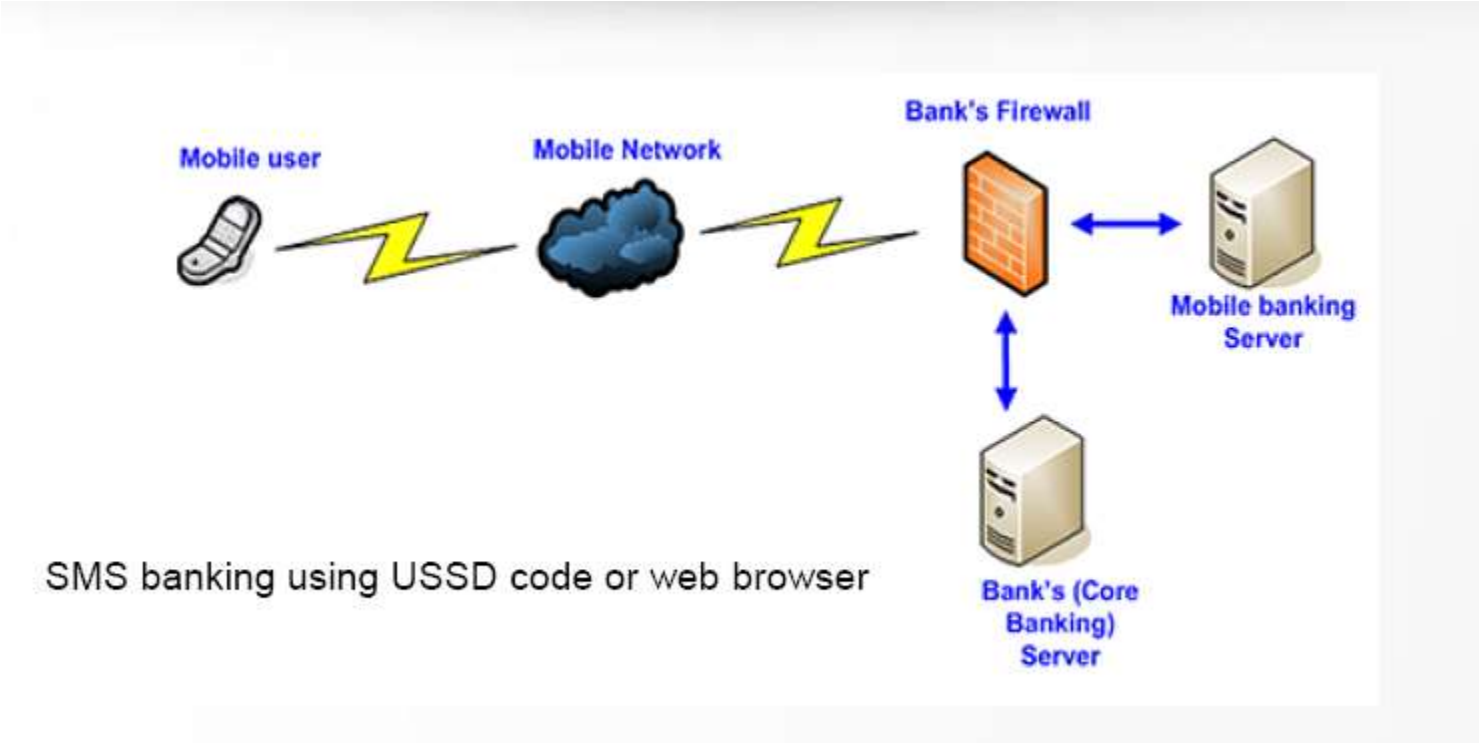
Apps

- Software designed for particular mobile software – e.g. Android, iOS, Symbian
- Downloaded by user and provides interface to bank

Unstructured Supplementary Service Data (USSD)

- Specific to GSM network
- USSD is session oriented, unlike SMS
- Turnaround time is lower, there is no storage at phone level, works through all phones

USSD & SMS – way forward?



Comparison

	Security	Usability	Ease of Maintenance	Customer reach
STK	High	Medium	Low	Medium
WAP	High	High	High	Medium
Voice	Medium	Low	High	High
SMS	Low	Low	Low	Medium
USSD	Medium	High	High	High
Android	High	High	Medium	Low
Apple	High	High	Medium	Low
Blackberry	High	High	Medium	Low

Mobile Banking Risks

- Mobile phones used for banking are on the rise, but mobile security is proving increasingly challenging for banks and service providers , as controls put in place to protect traditional online banking do not translate well when applied to mobile

Security and operational aspects

- Services should be available across all mobile networks
- Interoperability must between banks and mobile service operators and use formats like ISO 8583
- Mobile transactions permitted though validation through 2 factor authentications
- One of the factors to be mPIN
- End to end encryption when mPIN is used
- Proper encryption & security at all levels of processing

Mobile Banking Security

- Device level- Virus/ Worm/ Trojan/ Spyware
  Phishing/ Botnet
- Communication level- WPKI- Components- Certification /Validation/ Registration authority, Certificate repository, Digital certificate, Digital signature
- Application level-, MANET- Operates without using station, one router and gateway which will connect to cellular network . This may be used for Financial Inclusion also.
- Role of Mobile Service provider- Developing application, Integrator- sending information received from customer to bank end.

Security measures in Mobile Banking

- Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application
- Authentication of the device with a service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions
- User ID / Password authentication of bank's customer
- Two-factor authentication through mPIN or higher standard and end-to-end encryption of mPIN is desirable
- The mPIN shall be stored in a secure environment.
- Encryption of the data being transmitted over the air.
- Risk mitigation measures- Transaction limits and velocity, 2 factor authentication ,Grievance redressal mechanism

Recommendations

- Simplification of customer registration for mobile banking
- M-Pin generation may be simplified and standardized
- Banks to implement multiple channels (applications, SMS, USSD) and give options
- Bank specific USSD solutions and common USSD gateway
- MNOs to support STK related solutions

Thank You

ppatel@rbi.org.in